UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/624,481	07/23/2003	Makoto Fujiwara	60188-593	7409

7590 03/18/2009

Jack Q. Lever, Jr.
McDERMOTT, WILL & EMERY
600 Thirteenth Street, N.W.
Washington, DC 20005-3096

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
03/18/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/624,481	FUJIWARA ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *RCE filed on 01/28/2009*.

2a)☐ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11 and 18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *9 and 11* is/are allowed.

6)☒ Claim(s) *1-8, 10 and 18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 01/28/2009, has been entered.

2. New claim 18 is added. Thus claims 1-11 and 18 are pending of which claims 1, 8-11 are independent. Independent claim 1 is amended.

3. In the previous final office action set forth, Independent claims 9 and 11 were allowed and the allowance is still maintained.

Priority

4. Receipt is acknowledged of papers submitted under 35 U.S.C. 119 (a)-(d), which papers have been placed of record in the file.

Response to Argument

5. Applicant's remark/arguments filed on January 28, 2009 regarding claims 1-7 have been considered but are moot in view of the new ground(s) of rejection. Furthermore, applicant's remark/argument filed on January 28, 2009 regarding claims 8 and 10 have been fully considered but are not persuasive.

Referring to Independent claims 8 and 10, Applicant's representative argued that the reference/s on the record, does not disclose/teach some of the limitation recited in the claims.

Examiner disagrees with the above argument.

Examiner would like to point out that regarding claims 8 and 10, the art on the record disclosed what is recited in the claims. For the purpose of clarity, examiner would show how each limitation in the claims is taught by the reference as follows,

For instance regarding independent claims 8 and 10 Lin, the art on the record, discloses a program development supporting system for supporting development of an encrypted program, *[Paragraph 0012]* **Comprising**

a development LSI device having the same structure as that of an LSI device on which the encrypted program runs *[Paragraph 0012]***; and**

an external memory for storing a raw (binary) program, wherein the development LSI device includes a secure memory for storing encrypted common key information regarding a raw common key which is implemented in the LSI device in advance, *[See paragraph 0017-0018 the common key information regarding a raw common key which is met to be "the development parameter (338)" and "device identifier information" are stored/implemented in advance in every LSI device. See for instance "stores a hash of the development parameter (338), which meets the limitation of "encrypted common key information" for use with subsequently loaded versions of the software. This hash is stored in non volatile memory on the LSI device and see also the device identifier which is already implemented/stored in every*

mobile device in advance. See also how using these encrypted common key information, the software is authenticated before it is executed on LSI device**] and the development LSI device is capable of executing a first step of obtaining the raw common key from the common key information stored in the secure memory, and a second step of encrypting the raw (binary) program input from the external memory using the raw common key.** *[Paragraph 0016-0017]*

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

7. **Claims 8 and 10** are rejected under 35 U.S.C. 102(e) as being anticipated by Lin et al (hereinafter referred as Lin) (U.S. Publication No. 2002/0078380 A1) (filed on 12/20/2000).

8. **As per independent claims 8 and 10 Lin discloses a program development supporting system for supporting**

development of an encrypted program, *[Paragraph 0012]* **Comprising**

a development LSI device having the same structure as that of an LSI device on which the encrypted program runs *[Paragraph 0012]*; **and**

an external memory for storing a raw (binary) program, wherein the development LSI device includes a secure memory for storing encrypted common key information regarding a raw common key which is implemented in the LSI device in advance, *[See paragraph 0017-0018 the common key information regarding a raw common key which is met to be "the development parameter (338)" and "device identifier information" are stored/implemented in advance in every LSI device. See for instance "stores a hash of the development parameter (338), which meets the limitation of "encrypted common key information" for use with subsequently loaded versions of the software. This hash is stored in non volatile memory on the LSI device and see also the device identifier which is already implemented/stored in every mobile device in advance. See also how using these encrypted common key information, the software is authenticated before* it is executed on LSI device**] and the development LSI device is capable of executing a first step of obtaining the raw common key from the common key information stored in the secure memory, and a second step of encrypting the raw (binary) program input from the external memory using the raw common key.** *[Paragraph 0016-0017]*

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. **Claims 1-7 and 18** are rejected under 35 U.S.C. 103(a) as being unpatentable over Lin et al (hereinafter referred as **Lin)** (U.S. Publication No. 2002/0078380 A1) (filed on 12/20/2000) in view of Nelson (hereinafter referred as **"Nelson")** (US Patent Number: 7,299,203 B1) (filed on April 19, 2001)

11. **As per independent claims 1, dependent claim 2, 18 Lin discloses a method for developing a program which is to be installed in a system having an LSI device** [figure 1, ref. Num "104"], **the LSI device having a secure memory which includes an unrewritable area** [paragraph 0008] , **the method comprising the steps of:**

providing another LSI device having the same structure as that of the LSI device [Figure 1, ref. Num "108" and paragraph 0009]; **setting the provided LSI device to a development mode based on an inherent key information which is implemented in the LSI device in advance**[*See paragraph 0017-0018 the inherent key information which is*

met to be "the development parameter (338)" and "device identifier information" are stored/implemented in advance in every LSI device. See for instance "stores a hash of the development parameter (338) for use with subsequently loaded versions of the software. This hash is stored in non volatile memory on the LSI device and see also the device identifier which is already implemented/stored in every mobile device in advance. See also how using these inherent key information, the software is authenticated before it is executed on LSI device] **so that the provided LSI device is used as a development LSI device, the development mode being different from a product operation mode employed at the times of program installation and product operation; and developing the program on the development LSI device.** [Abstract, paragraph 0014 and paragraph 0016-0018 and claim 1]

Lin is silent about the following underlined amended limitation recited as "the setting the provided LSI device to a development mode based on an inherent and ***permanent key*** *information, which is implemented in the* ***unrewritable*** *area of the LSI device..."*

However, in the field of endeavor **Nelson,** discloses the following limitation which meets the above limitation.

- "FIG. 3c is a flowchart illustrating a process whereby an encrypted configuration program is loaded into an IC and decrypted by an on-chip decryptor according to a third embodiment. In step 302c, a primary configuration program is encrypted using algorithm A. In step 304c, the encrypted configuration program is loaded into the IC as a bitstream. In

step 306c, a decryption program A is also loaded into the IC. Algorithm A and decryption program A can be any commercially available encryption algorithm and decryption program or a proprietary encryption system developed by the customer. In step 308c the device is assembled into a customer system (PCB board) at their factory and the decryption keys are stored in a small externally WRITE ONLY memory location that is backed up by a small externally connected battery. In step 310c, upon in-system initialization, the decryption program A is executed. In step 312c, the decryption program A extracts the stored bitstream, decrypts it using the INTERNALLY READABLE keys, and internally recreates the configuration program. Lastly, in step 314c the IC is initialized for operation with the decrypted program. **As the key storage memory is not externally accessible, the keys remain secret and the configuration program IP is secure, meets the limitation recited as** setting the provided device to a development mode based on an inherent and permanent key information, which is implemented in the unrewritable area/secure area of a device.

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to add the features such as "the setting the provided device to a development mode based on an inherent and permanent key information, which is implemented in the unrewritable area of the device" as per teachings Nelson into the method as taught by Lin, in order to enhance the security of the system.

12. **As per dependent claims 3 the combination of Lin and Nelson discloses a method as applied to claims above. Furthermore Lin discloses the method further comprising the step of encrypting the program developed on the development LSI device at the program development step.** *[Paragraph 0012 and 0017]*

13. **As per dependent claims 4 the combination of Lin and Nelson discloses a method as applied to claims above. Furthermore Lin discloses the method wherein the operation of the LSI device is restricted such that when being set to the development mode, the LSI device cannot generate a key for encrypting a raw (binary) program.** *[Paragraph 0016-0017]*

14. **As per dependent claims 5-7 the combination of Lin and Nelson discloses a method as applied to claims above. Furthermore Lin discloses the method further comprising the steps of.' providing an LSI device having the same structure as that of the LSI device; setting the provided LSI device to a key-generation mode so that the provided LSI device is used as an key-generation LSI device, the key-generation mode being different from the development mode and the product operation mode; and installing an encrypted key-generation program in the key-generation LSI device and executing the key-generation program to generate a key.**[Paragraph 0012 and 0016-0018 and claim 1]

Allowable Subject Matter

15. Claims 9 and 11 **were allowed in the previous office action** and the allowance is still maintained.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

03/10/2009

/Samson B Lemma/

Examiner, Art Unit 2432

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434